

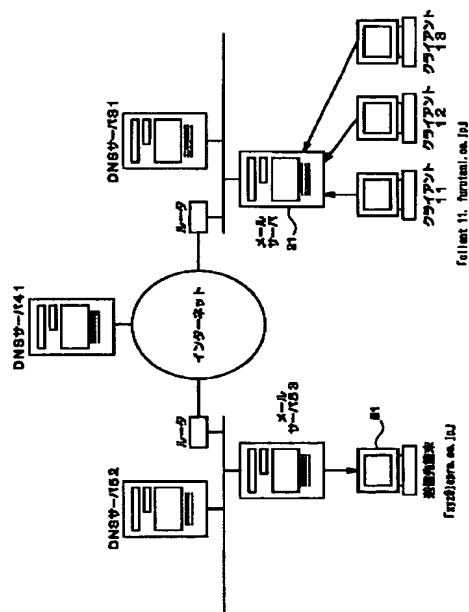
(11)Publication number : 2002-171286
(43)Date of publication of application : 14.06.2002

(71)Applicant : JEPRO:KK
(72)Inventor : OGURA OSAMU
SEIRO MIKITO

The diagram illustrates a network topology. A central circular hub is connected to several nodes. On the left, a node labeled '101-48BNC' is connected. On the right, a node labeled '101-48BNC' is connected. Below the hub, a node labeled '101-48BNC' is connected. To the right of the hub, a node labeled '101-48BNC' is connected. Further to the right, a node labeled '101-48BNC' is connected. At the bottom right, a node labeled '101-48BNC' is connected. The diagram shows a central hub connected to multiple nodes, representing a network topology.

<http://www19.ipdl.jpo.go.jp/PA1/result/detail/main/wAAA9KaOsjDA414171286P1.htm> 03/08/25

(11)特許出願公開番号



【特許請求の範囲】

【請求項1】インターネットに接続可能な端末装置と、当該端末装置と通信可能に接続されている通信中継装置と、当該通信中継装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた1または複数の宛先検索装置を備えた宛先検索システムと、を備えたネットワークシステムであって、前記宛先検索システム内の少なくとも1の前記宛先検索装置は、前記アドレステーブルに判定情報を関連づけて通信情報が記録されている通信情報テーブルを備えた通信情報検索装置であり、前記端末装置は、ドメイン名を、前記通信中継装置に送信し、前記通信中継装置は、前記端末装置から受信したドメイン名を、前記宛先検索システムに送信し、前記宛先検索システムは、前記アドレステーブルに基づいて、前記通信中継装置から受信したドメイン名をIPアドレスに変換するIPアドレス変換処理を行って、当該IPアドレスを前記通信中継装置に送信し、前記通信中継装置は、前記宛先検索システムから受信したIPアドレスに基づき前記判定情報を生成して、当該判定情報を前記宛先検索システムに送信し、前記宛先検索システムは、前記通信情報テーブルに、前記通信中継装置から受信した前記判定情報が記録されているならば、当該判定情報を前記通信情報に変換する通信情報変換処理を行って、当該通信情報を前記通信中継装置に送信すること、を特徴とするネットワークシステム。

【請求項2】インターネットに接続可能な端末装置と、当該端末装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた1または複数の宛先検索装置を備えた宛先検索システムと、を備えたネットワークシステムであって、前記宛先検索システム内の少なくとも1の前記宛先検索装置は、前記アドレステーブルに判定情報を関連づけて通信情報が記録されている通信情報テーブルを備えた通信情報検索装置であり、前記端末装置は、ドメイン名を、前記宛先検索システムに送信し、前記宛先検索システムは、前記アドレステーブルに基づいて、前記端末装置から受信したドメイン名をIPアドレスに変換するIPアドレス変換処理を行って、当該IPアドレスを前記端末装置に送信し、前記端末装置は、前記宛先検索システムから受信したIPアドレスに基づき前記判定情報を生成して、当該判定情報を前記宛先検索システムに送信し、前記宛先検索システムは、前記通信情報テーブルに、前

記端末装置から受信した前記判定情報が記録されているならば、当該判定情報を前記通信情報に変換する通信情報変換処理を行って、当該通信情報を前記端末装置に送信すること、を特徴とするネットワークシステム。

【請求項3】端末装置、およびドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた1または複数の宛先検索装置を備えた宛先検索システムと、通信可能に接続されている通信中継装置であって、前記宛先検索システム内の少なくとも1の前記宛先検索装置は、前記アドレステーブルに判定情報を関連づけて通信情報が記録されている通信情報テーブルを備えた通信情報検索装置であり、前記端末装置からドメイン名を受信して、当該ドメイン名を前記宛先検索システムに送信し、前記宛先検索システムによるIPアドレス変換処理により得られたIPアドレスを、前記宛先検索システムから取得し、前記宛先検索システムから受信したIPアドレスに基づき前記判定情報を生成して、当該判定情報を前記宛先検索システムに送信し、前記宛先検索システムによる通信情報変換処理により得られた前記通信情報を、前記宛先検索システムから取得することを特徴とする通信中継装置。

【請求項4】ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた1または複数の宛先検索装置を備えた宛先検索システムと、通信可能に接続されている端末装置であって、前記宛先検索システム内の少なくとも1の前記宛先検索装置は、前記アドレステーブルに判定情報を関連づけて通信情報が記録されている通信情報テーブルを備えた通信情報検索装置であり、ドメイン名を前記宛先検索システムに送信し、前記宛先検索システムによるIPアドレス変換処理により得られたIPアドレスを、前記宛先検索システムから取得し、前記宛先検索システムから受信したIPアドレスに基づき前記判定情報を生成して、当該判定情報を前記宛先検索システムに送信し、前記宛先検索システムによる通信情報変換処理により得られた前記通信情報を、前記宛先検索システムから取得することを特徴とする端末装置。

【請求項5】端末装置または通信中継装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた1または複数の宛先検索装置を備えた宛先検索システムであって、少なくとも1の前記宛先検索装置は、前記アドレステーブルに判定情報を関連づけて通信情報が記録されている通信情報テーブルを備えた通信情報検索装置であり、

10

20

30

40

50

前記端末装置または通信中継装置から、ドメイン名を取得し、
 前記アドレステーブルに基づいて、当該ドメイン名をIPアドレスに変換するIPアドレス変換処理を行って、当該IPアドレスを前記端末装置または通信中継装置に送信し、
 前記端末装置または通信中継装置が当該IPアドレスに基づき生成した前記判定情報を、前記端末装置または通信中継装置から取得し、
 前記通信情報テーブルに、当該判定情報が記録されているならば、当該判定情報を前記通信情報に変換する通信情報変換処理を行って、当該通信情報を前記端末装置または通信中継装置に送信すること、
 を特徴とする宛先検索システム。
 【請求項6】請求項1ないし請求項5のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記通信情報検索装置は、複数の内部ネットワークにおける端末装置または通信中継装置に関する判定情報または通信情報を記録している通信情報テーブルを備えていることを特徴とするもの。
 【請求項7】請求項1ないし請求項6のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記通信情報検索装置は、前記宛先検索装置から前記判定情報を取得して、前記通信情報変換処理を行うことを特徴とするもの。
 【請求項8】請求項1ないし請求項7のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記通信情報は、通信を許可するIPアドレスを含んでおり、
 前記通信中継装置または端末装置は、当該IPアドレスに基づいて、通信を行うことを特徴とするもの。
 【請求項9】請求項1ないし請求項7のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記通信情報は、通信不可能なIPアドレスを含んでいることを特徴とするもの。
 【請求項10】請求項1ないし請求項9のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記通信情報は、テキスト情報を含んでおり、
 前記通信中継装置または端末装置は、当該テキスト情報を操作者に提示することを特徴とするもの。
 【請求項11】請求項1ないし請求項10のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記宛先検索システムは、前記通信情報テーブルに前記判定情報が記録されていないときは、通信不可情報を前

記通信中継装置または端末装置に送信し、
 前記通信中継装置または端末装置は、当該通信不可情報を受信したときは、通信を行わないことを特徴とするもの。
 【請求項12】請求項1ないし請求項11のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記通信中継装置または端末装置は、前記端末装置の情報に基づいて、前記判定情報を生成することを特徴とするもの。
 【請求項13】請求項1ないし請求項12のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記通信中継装置または端末装置は、ユーザ情報に基づいて、前記判定情報を生成することを特徴とするもの。
 【請求項14】請求項1ないし請求項13のネットワークシステム、通信中継装置、端末装置または宛先検索システムにおいて、
 前記通信中継装置または端末装置は、前記宛先検索システムから受信したIPアドレスに、所定の情報を付加することにより、前記判定情報を生成することを特徴とするもの。
 【請求項15】インターネットに接続可能な端末装置と、
 当該端末装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた宛先検索装置と、
 前記端末装置および宛先検索装置と通信可能に接続されている通信中継装置と、
 を備えたネットワークシステムであって、
 前記宛先検索装置は、さらに、通信を許可または禁止するIPアドレスが記録されている通信許可テーブルを備え、
 前記端末装置は、ドメイン名を、前記通信中継装置に送信し、
 前記通信中継装置は、前記端末装置から受信したドメイン名を、前記宛先検索装置に送信し、
 前記宛先検索装置は、前記アドレステーブルに基づいて、またはインターネット上の他の宛先検索装置に問い合わせ、前記通信中継装置から受信したドメイン名をIPアドレスに変換し、
 前記宛先検索装置は、当該IPアドレスが、前記通信許可テーブルに記録されているか否かを判断することにより、通信許可の決定を行うことを特徴とするネットワークシステム。
 【請求項16】インターネットに接続可能な端末装置と、
 当該端末装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた宛先検索装置と、

を備えたネットワークシステムであって、
前記宛先検索装置は、さらに、通信を許可または禁止するIPアドレスが記録されている通信許可テーブルを備え、
前記端末装置は、ドメイン名を、前記宛先検索装置に送信し、
前記宛先検索装置は、前記アドレステーブルに基づいて、またはインターネット上の他の宛先検索装置に問い合わせ、前記端末装置から受信したドメイン名をIPアドレスに変換し、
前記宛先検索装置は、当該IPアドレスが、前記通信許可テーブルに記録されているか否かを判断することにより、通信許可の決定を行うことを特徴とするネットワークシステム。

【請求項17】 端末装置および通信中継装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた宛先検索装置であって、
さらに、通信を許可または禁止するIPアドレスが記録されている通信許可テーブルを備え、
前記アドレステーブルに基づいて、またはインターネット上の他の宛先検索装置に問い合わせ、前記通信中継装置または端末装置から受信したドメイン名をIPアドレスに変換し、
当該IPアドレスが、前記通信許可テーブルに記録されているか否かを判断することにより、通信許可の決定を行うことを特徴とする宛先検索装置。

【請求項18】 請求項1ないし請求項17のネットワークシステム、通信中継装置、端末装置、宛先検索システムまたは宛先検索装置において、
前記通信中継装置は、メールサーバ、ニュースサーバ、WWWサーバまたはプロキシサーバであることを特徴とするもの。

【請求項19】 情報発信装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた発信側の宛先検索装置と、
情報受信装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた受信側の宛先検索装置と、
を備えたネットワークシステムであって、
受信側の前記宛先検索装置は、さらに、通信を許可または禁止するIPアドレスが記録されている通信許可テーブルを備え、
発信側の前記宛先検索装置は、ドメイン名と前記情報発信装置のIPアドレスを受信側の前記宛先検索装置に送信して、前記情報受信装置のIPアドレスを問い、
受信側の前記宛先検索装置は、発信側の前記宛先検索装置から受信した前記情報発信装置のIPアドレスが、前記通信許可テーブルに記録されているか否かを判断する

ことにより、前記情報受信装置に対する通信許可の決定を行うことを特徴とするネットワークシステム。

【請求項20】 請求項19のネットワークシステムにおいて、

受信側の前記宛先検索装置は、通信を許可するときのみ、前記アドレステーブルに基づいて、発信側の前記宛先検索装置から受信したドメイン名をIPアドレスに変換し、当該IPアドレスを発信側の前記宛先検索装置に送信することを特徴とするもの。

- 10 【請求項21】 インターネットに接続可能な端末装置と、
当該端末装置と通信可能に接続されている通信中継装置と、
当該通信中継装置と通信可能に接続されている宛先検索システムと、
を用いて実現するインターネット通信管理方法であって、
前記端末装置において、ドメイン名を、前記通信中継装置に送信させ、
20 前記通信中継装置において、当該ドメイン名を、前記宛先検索システムに送信させ、
前記宛先検索システムにおいて、当該ドメイン名をIPアドレスに変換させて、当該IPアドレスを前記通信中継装置に送信させ、
前記通信中継装置において、当該IPアドレスに基づき判定情報を生成させて、当該判定情報を前記宛先検索システムに送信させ、
前記宛先検索システムにおいて、当該判定情報を通信情報に変換させて、当該通信情報を前記通信中継装置に送信させること、
30 を特徴とするインターネット通信管理方法。

- 【請求項22】 インターネットに接続可能な端末装置と、
当該端末装置と通信可能に接続されている通信中継装置と、
当該通信中継装置と通信可能に接続されている宛先検索装置と、
当該宛先検索装置とインターネットを介して接続されている通信情報検索装置と、
40 を用いて実現するインターネット通信管理方法であって、
前記端末装置において、ドメイン名を、前記通信中継装置に送信させ、
前記通信中継装置において、当該ドメイン名を、前記宛先検索装置に送信させ、
前記宛先検索装置において、当該ドメイン名をIPアドレスに変換させて、当該IPアドレスを前記通信中継装置に送信させ、
前記通信中継装置において、当該IPアドレスに基づき判定情報を生成させて、当該判定情報を前記宛先検索装

置に送信させ、
前記宛先検索装置において、当該判定情報を前記通信情報検索装置に送信させ、
前記通信情報検索装置において、当該判定情報を通信情報に変換させて、当該通信情報を前記宛先検索装置に送信させ、
前記宛先検索装置において、当該通信情報を前記通信中継装置に送信させること、
を特徴とするインターネット通信管理方法。

【請求項23】インターネットに接続可能な端末装置と、
当該端末装置と通信可能に接続されており、通信を許可または禁止するIPアドレスを記録している宛先検索装置と、
前記端末装置および宛先検索装置と通信可能に接続されている通信中継装置と、
を用いて実現するインターネット通信管理方法であって、
前記端末装置において、ドメイン名を、前記通信中継装置に送信させ、
前記通信中継装置において、当該ドメイン名を、前記宛先検索装置に送信させ、
前記宛先検索装置において、当該ドメイン名をIPアドレスに変換させ、当該IPアドレスに基づいて、通信許可の決定を行わせることを特徴とするネットワークシステム。

【請求項24】コンピュータを、通信中継装置または端末装置として機能させるプログラムを記録した記録媒体であって、
コンピュータに、宛先検索システムから受信したIPアドレスに基づき判定情報を生成させ、当該判定情報を宛先検索システムに送信するプログラムを記録した記録媒体。

【請求項25】請求項24のプログラムを記録した記録媒体であって、
コンピュータに、前記端末装置の情報に基づいて、前記判定情報を生成させるプログラムを記録しているもの。

【請求項26】ドメイン名を記録する領域と、
ドメイン名に関連づけて、IPアドレスを記録する領域と、
を備えているIPアドレスデータを記録した記録媒体において、
判定情報を記録する領域と、
判定情報を関連づけて、通信を許可するIPアドレスを記録する領域と、
を備えていることを特徴とするIPアドレスデータを記録した記録媒体。

【請求項27】ドメイン名を記録する領域と、
ドメイン名に関連づけて、IPアドレスを記録する領域と、

を備えているIPアドレスデータを記録した記録媒体において、
判定情報を記録する領域と、
判定情報を関連づけて、通信不可能なIPアドレスを記録する領域と、を備えていることを特徴とするIPアドレスデータを記録した記録媒体。

【請求項28】請求項26または請求項27のIPアドレスデータを記録した記録媒体において、
前記通信不可能なIPアドレスに関連づけて、テキスト情報を記録する領域を備えているもの。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、インターネットを用いて、情報通信を行うシステムに関するものである。

【0002】

【従来の技術】従来、インターネット上の通信相手を限定する方法として、図17のようなファイアウォールシステムがある。

【0003】これは、インターネットと内部ネットワークの間に、ファイアウォールサーバ104を設けて、内部ネットワークのクライアント101～103やメールサーバ105、プロキシサーバ106からの通信要求をすべて監視するものである。このファイアウォールサーバ104には、あらかじめ通信要求に対して、「通信を許可／不許可を判定するための情報」が登録されている。

【0004】例えば、クライアント101が、プロキシサーバ106を経由してWWWサーバ107に通信しようとする場合に、ファイアウォールサーバ104がそれを検知し、上記の「通信を許可／不許可を判定するための情報」に基づいて、その通信の許可を決定する。

【0005】同様に、クライアント102が、メールサーバ105を経由してメールサーバ108と通信しようとする場合に、ファイアウォールサーバ104がそれを検知し、その通信の許可を決定する。

【0006】このようなシステムを採用すれば、クライアント101～103の通信相手を限定することができる。

【0007】

【発明が解決しようとする課題】しかしながら、上記のような方法では、通信の許可／不許可を判定するための情報と、当該情報に基づいて通信の許可／不許可を判定するソフトウェアを備えたプロキシサーバ104を設けたネットワークを構築する必要があり、非常に面倒である。

【0008】また、上記のファイアウォールサーバ104で通信相手を限定するためには、通信プロトコル（例えば、WWWサーバ用にはHTTP、電子メール用にはSMTP）ごとに通信を許可もしくは不許可できるよう

ような仕組みを組み込む必要がある。これは、非常に面倒であるばかりでなく、今後新たに開発されるであろうプロトコルに対しては、対処することができない。

【0009】したがって、このような問題を解決して、クライアントの通信相手を、容易かつ効率的に規制するネットワークシステムを提供することを目的とする。

【0010】

【課題を解決するための手段および発明の効果】(1)

この発明のネットワークシステムは、インターネットに接続可能な端末装置と、当該端末装置と通信可能に接続されている通信中継装置と、当該通信中継装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた1または複数の宛先検索装置を備えた宛先検索システムとを備えており、前記宛先検索システム内の少なくとも1の前記宛先検索装置は、前記アドレステーブルに判定情報を関連づけて通信情報が記録されている通信情報テーブルを備えた通信情報検索装置であり、前記端末装置は、ドメイン名を、前記通信中継装置に送信し、前記通信中継装置は、前記端末装置から受信したドメイン名を、前記宛先検索システムに送信し、前記宛先検索システムは、前記アドレステーブルに基づいて、前記通信中継装置から受信したドメイン名をIPアドレスに変換するIPアドレス変換処理を行って、当該IPアドレスを前記通信中継装置に送信し、前記通信中継装置は、前記宛先検索システムから受信したIPアドレスに基づき前記判定情報を生成して、当該判定情報を前記宛先検索システムに送信し、前記宛先検索システムは、前記通信情報テーブルに、前記通信中継装置から受信した前記判定情報が記録されているならば、当該判定情報を前記通信情報に変換する通信情報変換処理を行って、当該通信情報を前記通信中継装置に送信することを特徴としている。

【0011】(2) この発明のネットワークシステム

は、インターネットに接続可能な端末装置と、当該端末装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた1または複数の宛先検索装置を備えた宛先検索システムとを備えており、前記宛先検索システム内の少なくとも1の前記宛先検索装置は、前記アドレステーブルに判定情報を関連づけて通信情報が記録されている通信情報テーブルを備えた通信情報検索装置であり、前記端末装置は、ドメイン名を、前記宛先検索システムに送信し、前記宛先検索システムは、前記アドレステーブルに基づいて、前記端末装置から受信したドメイン名をIPアドレスに変換するIPアドレス変換処理を行って、当該IPアドレスを前記端末装置に送信し、前記端末装置は、前記宛先検索システムから受信したIPアドレスに基づき前記判定情報を生成して、当該判定情報を前記宛先検索システムに送信し、前記宛先検索システムは、前記通信情報テーブルに、前記端末装置から受信した前記

判定情報が記録されているならば、当該判定情報を前記通信情報に変換する通信情報変換処理を行って、当該通信情報を前記端末装置に送信することを特徴としている。

【0012】したがって、宛先検索装置として、例えば、既存のDNS (Domain Name System) サーバを採用し、そのアドレステーブルに、判定情報と、通信情報として通信を許可するIPアドレスを記録すれば、端末装置、通信中継装置の通信相手先を規制することができる。また、そのアドレステーブルに、通信情報として通信不可能なIPアドレスを記録することによっても、端末装置等の通信相手先を規制することができる。

【0013】(6) この発明のネットワークシステムは、前記通信情報検索装置は、複数の内部ネットワークにおける端末装置または通信中継装置に関する判定情報または通信情報を記録している通信情報テーブルを備えていることを特徴としている。

【0014】(7) この発明のネットワークシステムは、前記通信情報検索装置は、前記宛先検索装置から前記判定情報を取得して、前記通信情報変換処理を行うことを特徴としている。

【0015】したがって、システム管理者は、通信情報テーブルの通信情報等を操作することにより、一括して、複数の内部ネットワーク内の端末装置等の通信相手先を規制することができる。

【0016】(8) この発明のネットワークシステムは、前記通信情報は、通信を許可するIPアドレスを含んでおり、前記通信中継装置または端末装置は、当該IPアドレスに基づいて、通信を行うことを特徴としている。

【0017】(9) この発明のネットワークシステムは、前記通信情報は、通信不可能なIPアドレスを含んでいることを特徴としている。

【0018】したがって、システム管理者は、通信情報テーブルに通信を許可するIPアドレス等を記録することにより、通信中継装置等の通信を規制することができる。

【0019】(10) この発明のネットワークシステムは、前記通信情報は、テキスト情報を含んでおり、前記通信中継装置または端末装置は、当該テキスト情報を操作者に提示することを特徴としている。

【0020】したがって、操作者は、テキスト情報を閲覧することによって、通信が規制されたことや、通信が規制される期間等の通信情報に関する情報を知得することができる。

【0021】(11) この発明のネットワークシステムは、前記宛先検索システムは、前記通信情報テーブルに前記判定情報が記録されていないときは、通信不可情報を前記通信中継装置または端末装置に送信し、前記通信中継装置または端末装置は、当該通信不可情報を受信し

たときは、通信を行わないことを特徴としている。

【0022】したがって、システム管理者は、通信情報テーブルに判定情報を記録しないことにより、当該判定情報を生成する端末装置等の通信相手先を規制することができる。

【0023】(12) この発明のネットワークシステムは、前記通信中継装置または端末装置は、前記端末装置の情報に基づいて、前記判定情報を生成することを特徴としている。

【0024】したがって、端末装置ごとに通信相手先を規制することができる。

【0025】(13) この発明のネットワークシステムは、前記通信中継装置または端末装置は、ユーザ情報に基づいて、前記判定情報を生成することを特徴としている。

【0026】したがって、ユーザごとに、端末装置の通信相手先を規制することができる。

【0027】(14) この発明のネットワークシステムは、前記通信中継装置または端末装置は、前記宛先検索システムから受信したIPアドレスに、所定の情報を付加することにより、前記判定情報を生成することを特徴としている。

【0028】したがって、通信中継装置等は、容易に判定情報を生成することができる。

【0029】(15) この発明のネットワークシステムは、インターネットに接続可能な端末装置と、当該端末装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた宛先検索装置と、前記端末装置および宛先検索装置と通信可能に接続されている通信中継装置とを備えており、前記宛先検索装置は、さらに、通信を許可または禁止するIPアドレスが記録されている通信許可テーブルを備え、前記端末装置は、ドメイン名を、前記通信中継装置に送信し、前記通信中継装置は、前記端末装置から受信したドメイン名を、前記宛先検索装置に送信し、前記宛先検索装置は、前記アドレステーブルに基づいて、またはインターネット上の他の宛先検索装置に問い合わせ、前記通信中継装置から受信したドメイン名をIPアドレスに変換し、前記宛先検索装置は、当該IPアドレスが、前記通信許可テーブルに記録されているか否かを判断することにより、通信許可の決定を行うことを特徴としている。

【0030】したがって、宛先検索装置として、既存のDNSサーバを採用し、これに通信許可テーブルを格納して、通信許可の決定を行わせれば、端末装置等の通信相手先の規制を行うことができる。

【0031】(19) この発明のネットワークシステムは、情報発信装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた発信側の宛先検索装置と、情報受信

装置と通信可能に接続されており、ドメイン名に関連づけてIPアドレスが記録されているアドレステーブルを備えた受信側の宛先検索装置とを備えており、受信側の前記宛先検索装置は、さらに、通信を許可または禁止するIPアドレスが記録されている通信許可テーブルを備え、発信側の前記宛先検索装置は、ドメイン名と前記情報発信装置のIPアドレスを受信側の前記宛先検索装置に送信して、前記情報受信装置のIPアドレスを問い、受信側の前記宛先検索装置は、発信側の前記宛先検索装置から受信した前記情報発信装置のIPアドレスが、前記通信許可テーブルに記録されているか否かを判断することにより、前記情報受信装置に対する通信許可の決定を行うことを特徴としている。

【0032】(20) この発明のネットワークシステムは、受信側の前記宛先検索装置は、通信を許可するときのみ、前記アドレステーブルに基づいて、発信側の前記宛先検索装置から受信したドメイン名をIPアドレスに変換し、当該IPアドレスを発信側の前記宛先検索装置に送信することを特徴としている。

【0033】したがって、情報受信装置に送られてくる電子メール等の情報発信元を、規制することができる。

【0034】なお、この発明において、「宛先検索装置」とは、ドメイン名をIPアドレスに変換するものであり、下記の実施形態においては、DNSサーバ31、41、52(図1)、DNSサーバ131(図9)、DNSサーバ131、152(図13)、DNSサーバ514、521、532(図16)が該当する。

【0035】「通信情報検索装置」とは、通信情報テーブルを備えた宛先検索装置であり、下記の実施形態においては、DNSサーバ41(図1)、DNSサーバ131(図9、図13)、DNSサーバ521(図16)が該当する。

【0036】「通信中継装置」とは、端末装置および宛先検索装置と通信可能に接続されているものであり、メールサーバ、ニュースサーバ、WWWサーバまたはプロキシサーバ、ビデオサーバ、IRC(チャット)サーバなど宛先検索システムを利用するものである。下記の実施形態においては、メールサーバ21(図1)、メールサーバ121(図13)、プロキシサーバ513(図16)が該当する。

【0037】「端末装置」とは、下記の実施形態においては、クライアント11~13(図1)、クライアント111、112(図9、13)、クライアント511~513(図16)が該当する。

【0038】「宛先検索システム」とは、1または複数の宛先検索装置を備えたネットワークであり、下記の実施形態においては、DNSサーバ31、41、52により構成されるネットワーク(図1)が該当する。また、それぞれ、DNSサーバ131(図9)、DNSサーバ131、152(図13)、DNSサーバ514、52

1, 532 (図16)により構成されるネットワークも該当する「判定情報」とは、端末装置等において生成されるものであり、下記の実施形態においては、IPアドレスにゾーン名を付加したもの(192.168.222.1.junior.など)が該当する。

【0039】「通信情報」とは、通信情報テーブルに記録されているものであり、下記の実施形態においては、DBファイルに登録された通信を許可するIPアドレス(192.168.222.1など)が該当する。なお、通信不可能なIPアドレスや、テキスト情報も含む概念である。

【0040】「IPアドレス変換処理」とは、ドメイン名をIPアドレスに変換する処理であり、下記の実施形態においては、図6aのST15、図7aのST33が該当する。

【0041】「通信情報変換処理」とは、判定情報を通信情報に変換する処理であり、下記の実施形態においては、図6bのST20、図7bのST39が該当する。

【0042】「アドレステーブル」とは、ドメイン名に関連づけて、IPアドレスが記録されているものであり、下記の実施形態においては、DNSサーバ31のDBファイル等が該当する。

【0043】「通信情報テーブル」とは、アドレステーブルに判定情報を関連づけて通信情報が記録されているものであり、下記の実施形態においては、DNSサーバ41(図1)、DNSサーバ131(図9、図13)、DNSサーバ521(図16)のDBファイルが該当する。

【0044】「通信許可テーブル」とは、通信を許可または禁止するIPアドレスが記録されているものであり、下記の実施形態においては、DNSサーバの通信アドレスデータベースが該当する。

【0045】「情報発信装置」とは、情報受信装置に対して情報を送信する装置であり、下記の実施形態においては、メールサーバ153が該当する。

【0046】「情報受信装置」とは、情報発信装置から情報を受信する装置であり、下記の実施形態においては、メールサーバ121が該当する。

【0047】「プログラム、データを記録した記録媒体」とは、フレキシブルディスク、CD-ROM、ハードディスク、メモ리카ード、ROM、バンチカード、テープ等を含む概念である。また、コンピュータによって直接実行可能なプログラムを記録した記録媒体だけでなく、一旦他の記録媒体(ハードディスク等)にインストールすることによって実行可能となるようなプログラムを記録した記録媒体や、暗号化されたり、圧縮されたりしたプログラムを記録した記録媒体を含む概念である。

【0048】

【発明の実施の形態】1 第一の実施形態

以下に、電子メールの送信先を規制するときの、ネットワークシステムの一実施形態を示す。

【0049】1.1 全体の構成、処理の概要

図1に、この発明の一実施形態におけるネットワークシステムの全体構成を示す。

【0050】クライアント11~13は、juniorゾーンに属し、メールサーバ21と通信可能に接続されている。メールサーバ21は、インターネットを介して、送信先メールサーバ53と通信可能に接続されている。また、メールサーバ21は、LAN(Local Area Network)を介してDNS(Domain Name System)サーバ31に接続されており、インターネットを介してjuniorゾーンに権威をもつDNSサーバ41に接続されている。このDNSサーバ41に格納されているDBファイル(ドメイン名からIPアドレスに変換するテーブル)には、通信を許可するIPアドレス(例えば、192.168.222.1)に、ゾーン名「.junior.」を付加したもの(例えば、192.168.222.1.junior.)が登録されている。以下に、このシステムの処理の概要を説明する。

【0051】クライアント11は、メールサーバ21に、ユーザが入力した送信先メールアドレス「xyz@jepr.o.co.jp」を送信して、送信先メールサーバ53のIPアドレスを、DNSサーバ31に問う。DNSサーバ31は、送信先DNSサーバ52にアクセスして、メールサーバ53のIPアドレスを取得し、これをメールサーバ21に返す。

【0052】メールサーバ21は、このIPアドレスにゾーン名「.junior.」を付加し、これが、DNSサーバ41のDBファイルに登録されているか否かを、DNSサーバ31に問う。DNSサーバ31はDNSサーバ41に問い合わせ、DNSサーバ41が登録されていると判断すると、DNSサーバ31を介して、メールサーバ21にメール送信を許可する。

【0053】このように、システム管理者は、DNSサーバ41のDBファイルの登録内容を変更することにより、クライアント11~13のメール送信先を規制することができる。

【0054】なお、クライアント51のメール送信先も、メールサーバ53がDNSサーバ41を用いて、規制することができる。すなわち、インターネット上の複数のネットワーク(または、クライアント)から発信されるメールの送信先を、DNSサーバ41を用いて規制することができる。

【0055】1.2 DNSサーバ31、DNSサーバ41のハードウェアの構成

図2に、図1に示すDNSサーバ31、DNSサーバ41のハードウェアの構成例を示す。CPU41aには、バスラインを介して、メモリ41b、ハードディスク41c、CD-ROMドライブ41dが接続されている。メモリ41bには、IPアドレス検索プログラム、DBファイル、システムプログラム(OS)などが登録されている。

【0056】IPアドレス検索プログラムは、インターネット上の他のDNSサーバに問い合わせたり、自己のDBファイルを利用して、ホスト名のIPアドレスを検索するもの（いわゆる「名前解決」を行うもの）である。

【0057】DBファイルには、各DNSサーバが権威をもつゾーン中のホスト名（左辺値）を、IPアドレス（右辺値）に変換するためのアドレスレコード（Aレコード）等が記述されている。さらに、DNSサーバ41のDBファイルのAレコードには、通信先として許可されるIPアドレスに「.junior.（ゾーン名）」を付加したもの（左辺値）と、そのIPアドレス（右辺値）が記述される（図3参照）。なお、IPアドレス検索プログラムは、システムプログラムと共同して、上記の機能を実行する。

【0058】1.3 メールサーバ21のハードウェアの構成

図4に、図1に示すメールサーバ21のハードウェアの構成例を示す。CPU21aには、バスラインを介して、メモリ21b、ハードディスク21c、CD-ROMドライブ21dが接続されている。ハードディスク21cには、メール配送プログラム（MTA: Message Transfer Agent）、スプールファイル、通信規制プログラム、システムプログラムなどが登録されている。

【0059】メール配送プログラムは、クライアントから受信した電子メールを送信先のメールサーバに配送するものである。スプールファイルには、受信したメール、送信するメールが書き込まれる。

【0060】通信規制プログラムは、DNSサーバに対して、ホスト名のIPアドレスを問うものである。また、DNSサーバから取得したIPアドレスに、ゾーン名を付加して、DNSサーバに対して、通信許可を問うものである。

【0061】なお、メール配送プログラム、通信規制プログラムは、システムプログラムと共同して、上記の機能を実行する。

【0062】1.4 クライアントのハードウェアの構成
図5に、図1に示すクライアント11のハードウェアの構成例を示す。CPU11aには、バスラインを介して、メモリ11b、ディスプレイ11c、キーボード11d、ハードディスク11e、CD-ROMドライブ11fが接続されている。

【0063】ハードディスク11eには、WWWサーバに接続するためのブラウザプログラム（例えば、マイクロソフト社のInternet Explorerなど）、メールプログラム（例えば、マイクロソフト社のOutlook Expressなど）、システムプログラム（例えば、マイクロソフト社のWindowsなど）などが登録されている。

【0064】なお、ブラウザプログラム、メールプログラムは、システムプログラムと共同して、上記の機能を

実行する。

【0065】1.5 フローチャート

図6a、bに、クライアント11が送信先端末51（メールアドレス: xyz@jepro.co.jp）にメール送信するときの、クライアント11、メールサーバ21、DNSサーバ31、DNSサーバ41、DNSサーバ51の処理を示す。

【0066】クライアント11は、メールサーバ21に、ユーザが入力した「xyz@jepro.co.jp」あての電子メールを送信する（ST11）。

【0067】メールサーバ21は、その電子メールをスプールファイルに書き込むとともに、xyz@jepro.co.jpからドメイン名「jepro.co.jp」を抜き出し、これをDNSサーバ31に送信して、jepro.co.jpドメインのメールサーバ53のIPアドレスを問う（ST12）。

【0068】DNSサーバ31は、jepro.co.jpドメインのDNSサーバ52にアクセスして、メールサーバ53のIPアドレスを問う（ST13）。DNSサーバ52は、メールサーバ53のホスト名を取得し（ST14）、これを、自己のDBファイル（図示せず）を用いてIPアドレス「192.168.222.1」に変換する（ST15）。DNSサーバ31は、このIPアドレスを取得すると、メールサーバ21に送信する（ST16）。

【0069】次に、メールサーバ21は、「192.168.222.1」にゾーン名「.junior.」を付加し、これが（192.168.222.1.junior.）、juniorゾーンに権威をもつDNSサーバ41のDBファイル（図3参照）に登録されているか否かを、DNSサーバ31を経由してDNSサーバ41に問う（ST17、18）。

【0070】DNSサーバ41は、登録されていると判断すると（ST19）、192.168.222.1.junior.をIPアドレス「192.168.222.1」に変換し（ST20）、これをDNSサーバ31を経由してメールサーバ21に送信する（ST21、22）。メールサーバ21は、そのIPアドレスに基づいて、スプールファイルの電子メールをメールサーバ53に送信する（ST25、26）。

【0071】また、ST19において、DNSサーバ41は、DBファイルに登録されていないと判断すると、DNSサーバ31を経由してメールサーバ21に対して、メール送信を禁止する指令を送る（ST23、24）。メールサーバ21は、メール送信が不可能である旨をクライアント11に送信する（ST25、27）。

1.6

なお、この実施形態においては、メールサーバ21に通信規制プログラムを格納して、メールサーバ21が判定情報（192.168.222.1.junior.）の生成を行っている

（ST17）。しかしながら、クライアント11に通信規制プログラムを格納して、クライアント11が判定情報を生成してもよい。図7a、bに、WWWサーバの接続先を規制する場合を一例として、クライアントが判定

情報を生成するときの処理を説明する。

【0072】クライアント11は、ユーザが入力した接続先URL「http://www.jepro.co.jp」からホスト名「www.jepro.co.jp」を抜き出し、これをDNSサーバ31に送信する(ST31)。

【0073】DNSサーバ31は、インターネット上の他のDNSサーバに問い合わせ、www.jepro.co.jpをIPアドレスに変換してもらう(ST32)。そして、DNSサーバ31は、IPアドレス「192.168.222.2」を取得すると(ST33、34)、これをクライアント11に送信する(ST35)。

【0074】クライアント11は、「192.168.222.2」にゾーン名「.junior.」を付加し(ST36)、これが(192.168.222.2.junior.)、juniorゾーンに権威をもつDNSサーバ41のDBファイル(図3参照)に登録されているか否かを、DNSサーバ31を経由してDNSサーバ41に問う(ST36、37)。

【0075】DNSサーバ41は、登録されていると判断すると、192.168.222.1.junior.をIPアドレス「192.168.222.2」に変換し(ST38、39)、これをDNSサーバ31を経由してクライアント11に送信する(ST40、41)。クライアント11は、そのIPアドレスに基づいて、WWWサーバに接続する(ST44、45)。

【0076】また、ST38において、DNSサーバ41は、DBファイルに登録されていないと判断すると、DNSサーバ31を経由してクライアント11に対して、通信を禁止する指令を送る(ST42、43)。クライアント11は、接続不可能である旨をディスプレイ11cに表示する(ST44、46)。

【0077】なお、クライアントと通信可能なプロキシサーバを設け、それに通信規制プログラムを格納してもよい。この場合、このプロキシサーバが、上記ST36等の処理を行う。

1.7

なお、この実施形態においては、メールサーバ21が、通信先のIPアドレスにゾーン名を付加して、DNSサーバ31に通信の許否を問うている。しかしながら、これに限られるものではなく、メールサーバ21が、ユーザの情報をクライアント11から取得して、ユーザの種別にそれぞれ所定の記号を付加すれば、ユーザの種別に通信相手の制限を設定することができる。例えば、教育機関における管理者、教師、児童別によって、所定の記号(管理者:manager、教師:teacher、児童:student)を設定し、図8に示すようなDBファイルを作成することによって、管理者、教師、児童別に通信相手を規制することができる。この例においては、児童に対してIPアドレス「192.161.112.1」への通信は許可しないが、管理者、教師に対しては通信を許可している。

【0078】また、通信相手の制限設定がそれぞれ異な

るDNSサーバを複数設けるようにしてもよい。この場合、クライアントが、ユーザの認証を行って、利用すべきDNSサーバを決定するようなソフトウェアを格納すれば、同じクライアントでありながら、ユーザによって通信相手の制限を変更することができる。

【0079】また、この実施形態においては、メールサーバ21が、通信先のIPアドレスにゾーン名を付加して、DNSサーバ31に通信の許否を問うている。しかしながら、これに限られるものではなく、メールサーバ21が、クライアントの識別情報をクライアント11から取得して、クライアント別にそれぞれ所定の記号を付加すれば、クライアントの種別に通信相手の制限を設定することができる。

【0080】また、この実施形態においては、クライアント11~13に対して通信を許可するIPアドレスを記録したDBファイルを、インターネット上のDNSサーバ41に備えている。しかしながら、これに限られるものではなく、当該DBファイルを内部ネットワーク内のDNSサーバ31に備えてもよい。

【0081】また、上記の実施形態においては、通信中継装置として、メールサーバ21を一例として説明している。しかしながら、これに限られるものではなく、通信中継装置は、情報提供サーバ(ニュースサーバ、WWWサーバなど)またはプロキシサーバであってもよい。

【0082】また、この実施形態では、DNSサーバ41のDBファイルに、判定情報(192.168.222.1.junior.)に対応づけて、通信を許可するIPアドレス(192.168.222.1)が記録されている(図3参照)。しかしながら、これに限られるものではなく、判定情報を対応付けて、通信不可能なIPアドレスを記録するものであってもよい。さらに、テキスト情報を記録するものであってもよい。このテキスト情報は、例えば、「通信が許可されていません」や「〇月〇日から△月△日まで、通信が許可されていません」というようなものである。この場合、クライアントが、ディスプレイにおいてテキスト情報を表示することにより、ユーザに対して、わかりやすく通信結果を提供することができる。

【0083】2 第二の実施形態

以下に、ウェブサイト装置の接続先を規制するときの、ネットワークシステムの一実施形態を示す。

【0084】2.1 全体の構成

図9に、この発明の一実施形態におけるネットワークシステムの全体構成を示す。

【0085】juniorゾーンに属するクライアント111、112は、LANを介して、メールサーバ121、juniorゾーンに権威をもつDNSサーバ131に接続されている。DNSサーバ131は、インターネットを介して、ウェブサイト装置141と接続されている。このDNSサーバ131は、ホスト名をIPアドレスに変換するためのDBファイルと、クライアント111、11

2に対して通信を許可するIPアドレスを登録したデータベースを格納している。

【0086】DNSサーバ131は、クライアント111が接続しようとするウェブサイト装置141のホスト名を受信すると、インターネット上の他のDNSサーバに問い合わせ、ウェブサイト装置141のIPアドレスを取得する。

【0087】そして、DNSサーバ131は、上記のデータベースに、ウェブサイト装置141のIPアドレスが登録されているか否かを判断する。登録されているならば、DNSサーバ131は、クライアント111に対して、ウェブサイト装置141への通信を許可する。

【0088】したがって、システム管理者は、DNSサーバ131のデータベースに登録するIPアドレスを変更等することで、クライアント111、112の通信相手を、容易に規制することができる。

【0089】2.2 DNSサーバ131のハードウェアの構成

図10に、図9に示すDNSサーバ131のハードウェアの構成例を示す。CPU131aには、バスラインを介して、メモリ131b、ハードディスク131c、CD-ROMドライブ131dが接続されている。メモリ131bには、IPアドレス検索プログラム、通信判定プログラム、DBファイル、通信アドレスデータベース、システムプログラム(OS)などが登録されている。

【0090】通信判定プログラムは、IPアドレス検索プログラムが検索したIPアドレスが、通信アドレスデータベースに登録されているか否かを判断するものである。通信アドレスデータベースには、システム管理者が通信を許可するIPアドレスが登録されている(図12参照)。なお、IPアドレス検索プログラムとDBファイルは、上記と同様である。

【0091】2.3 クライアント111のハードウェアの構成

上記1.4と同様である。

【0092】2.4 フローチャート

図11に、クライアント111がウェブサイト装置141のJEPROウェブサイト(URL: http://www.jepro.co.jp)に接続するときの、クライアント111のブラウザプログラム、DNSサーバ131のIPアドレス検索プログラム、通信判定プログラムの処理を示す。

【0093】クライアント111は、ユーザが入力した接続先URL「http://www.jepro.co.jp」からホスト名「www.jepro.co.jp」を抜き出し、これをDNSサーバ131に送信する(ST51)。

【0094】DNSサーバ131は、インターネット上の他のDNSサーバに問い合わせ、www.jepro.co.jpをIPアドレスに変換してもらう(ST52、53)。そして、DNSサーバ131は、ウェブサイト装置141のIPアドレス「192.168.222.2」を取得する(ST

54、55)。

【0095】次に、DNSサーバ131は、「192.168.222.2」が、図12に示す通信アドレスデータベースに登録されているか否かを判断する(ST56)。DNSサーバ131は、登録されていると判断すると、「192.168.222.2」をクライアント111に送信する(ST57)。つまり、ウェブサイト装置141への接続を許可するのである。

【0096】クライアント111は、「192.168.222.2」を用いて、JEPROウェブサイトへ接続する(ST59、60)。

【0097】また、ST56において、通信アドレスデータベースに登録されていないと判断すると、DNSサーバ131は、クライアント111に対して、通信を禁止する指令を送信する(ST58)。クライアント111は、ウェブサイト装置141への接続が不可能である旨をディスプレイに表示する(ST59、61)。

【0098】なお、この実施形態においては、クライアント111が、直接、DNSサーバ131に名前解決を要求している(ST51)。しかしながら、これに限られるものではなく、クライアント111からURLを取得したプロキシサーバ等が、DNSサーバ131に名前解決を要求するものであってもよい。

【0099】2.6 電子メールの送信先の規制

なお、この実施形態においては、ウェブサイト装置への通信規制を行うときを一例として説明している。しかしながら、電子メールの送信先を規制するものであってもよい。これを、クライアント111から端末151にメール送信する場合を一例として、図13の全体構成図、図14のフローチャートを用いて説明する。

【0100】クライアント111は、メールサーバ121に、ユーザが入力した「xyz@jepro.co.jp」あての電子メールを送信する(ST71)。

【0101】メールサーバ121は、その電子メールをスプールファイルに書き込むとともに、xyz@jepro.co.jpからドメイン名「jepro.co.jp」を抜き出し、これをDNSサーバ131に送信して、jepro.co.jpドメインのメールサーバ153のIPアドレスを問う(ST72)。

【0102】DNSサーバ131は、jepro.co.jpドメインのDNSサーバ152にアクセスして(ST73)、メールサーバ153のIPアドレスを問う。DNSサーバ152は、メールサーバ153のホスト名を取得して、それをIPアドレス「192.168.222.1」に変換する(ST74、75)。

【0103】DNSサーバ131は、DNSサーバ152からメールサーバ153のIPアドレス「192.168.222.1」を取得すると(ST76)、これが図12に示す通信アドレスデータベースに登録されているか否かを判断する(ST77)。

21

【0104】DNSサーバ131は、登録されていると判断すると、メールサーバ121に対して、送信先のメールサーバ153のIPアドレス「192.168.222.1」を送信する(ST78)。メールサーバ121は、スプールファイルの電子メールを、送信先メールサーバ153に送信する(ST80, 81)。

【0105】また、ST77において、DNSサーバ131は、登録されていないと判断すると、メールサーバ121に対して、メール送信を禁止する指令を送信する(ST79)。メールサーバ121は、メール送信が不可能である旨をクライアント111に送信する(ST80, 82)。

【0106】2.7 電子メール等の送信元の規制

なお、上記の実施形態2.6においては、クライアントのメール送信先を規制する場合について説明している。しかしながら、クライアントの電子メール等の送信元を規制する場合にも、このシステムを利用することができる。これを、端末151からクライアント111にメール送信する場合を一例として、図13の全体構成図、図15のプロチャートを用いて説明する。

【0107】DNSサーバ131は、送信元のDNSサーバ152から、メールサーバ121のIPアドレスを問われる際に(ST91, 92)、送信元のメールサーバ153のIPアドレスを取得する(ST93)。そして、送信元のメールサーバ153のIPアドレスが、図12に示す通信アドレスデータベースに登録されているか否かを判断する(ST94)。

【0108】登録されていると判断すると、DNSサーバ131は、メールサーバ121のホスト名を取得し、これを、DBファイルに基づいてIPアドレスに変換する(ST95, 96)。そして、DNSサーバ131は、メールサーバ121のIPアドレスを、送信元のDNSサーバ152に送信する(ST97)。

【0109】送信元のメールサーバ153は、DNSサーバ152から送信先のメールサーバ121のIPアドレスを取得して(ST98)、送信先のメールサーバ121に電子メールを送信する(ST100, 101)。

【0110】また、ST94において、DNSサーバ131は、登録されていないと判断すると、メール送信が不可能である旨を送信元のメールサーバ153に送信する(ST99)。

2.8

また、この実施形態においては、DNSサーバ131に通信判定プログラム等を備えて、DNSサーバ131が、通信の許可を判断している。しかしながら、これに限られるものではなく、メールサーバ121に通信判定プログラムと通信アドレスデータベースを備え、メールサーバ121が、DNSサーバ131からIPアドレスを取得して、通信の許可を判断してもよい。同様に、クライアントと通信可能に接続されているプロキシサーバ

22

が、通信の許可を判断してもよい。

【0111】また、この実施形態においては、DNSサーバ131の通信アドレスデータベースに通信を許可するIPアドレスを登録している。しかしながら、これに限られるものではなく、通信を禁止するIPアドレスを登録してもよい。

【0112】また、この実施形態においては、既存のDNSサーバに通信アドレスデータベース等を備えて、DNSサーバ131が通信の許可を判断している。しかしながら、これに限られるものではなく、DNSサーバとは別個の装置であって、通信アドレスデータベース等を備えた装置を設けて、それが通信の許可を判断するものであってもよい。

3

また、この発明においては、通信相手先のIPアドレスに基づいて、通信の許可/不許可を判定しているため、未知の通信プロトコル(新たに開発された通信プロトコル)に対しても、この発明を適用することができる。これを、第一の実施形態で述べたシステム(図16参照)において、未知の通信プロトコルを利用するクライアントが、未知機能サーバと通信しようとする場合を一例として説明する。

【0113】まず、クライアント511は、送信先未知機能サーバ531のドメイン名をプロキシサーバ513に送信して、未知機能サーバ531のIPアドレスを、DNSサーバ514に問う。DNSサーバ514は、DNSサーバ532にアクセスして、未知機能サーバ531のIPアドレスを取得し、これをプロキシサーバ513に返す。

【0114】プロキシサーバ513は、このIPアドレスにゾーン名を付加し、これが、DNSサーバ521のDBファイルに登録されているか否かを、DNSサーバ514に問う。DNSサーバ514はDNSサーバ521に問い合わせ、DNSサーバ521は登録されていると判断すると、DNSサーバ514を介して、プロキシサーバ513に通信を許可する。

【0115】このように、このシステムを利用すれば、通信プロトコルごとに通信の許可/不許可を判定していたため、未知の通信プロトコルには対処できない従来のファイアウォールサーバとは異なり、未知の通信プロトコルに対しても、通信の許可/不許可を判定できる。

【0116】なお、第二の実施形態で述べたシステムを採用しても、未知の通信プロトコルに対して、通信の許可/不許可を判定できる。

【図面の簡単な説明】

【図1】一実施形態におけるネットワークシステムの全体構成を示す図である。

【図2】一実施形態におけるDNSサーバ31のハードウェアの構成を示す図である。

【図3】一実施形態におけるDNSサーバ31のDBフ

ファイルを示す図である。

【図4】一実施形態におけるメールサーバ21のハードウェアの構成を示す図である。

【図5】一実施形態におけるクライアント11のハードウェアの構成を示す図である。

【図6a】一実施形態において、電子メールの送信先を規制するときのフローチャートである。

【図6b】一実施形態において、電子メールの送信先を規制するときのフローチャートである。

【図7a】一実施形態において、WWWサーバの接続先を規制するときのフローチャートである。

【図7b】一実施形態において、WWWサーバの接続先を規制するときのフローチャートである。

【図8】一実施形態におけるDNSサーバ31のDBファイルを示す図である。

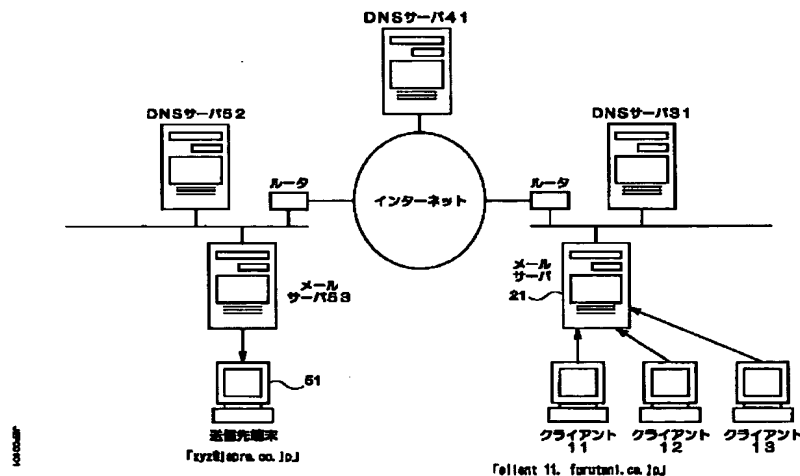
【図9】一実施形態におけるネットワークシステムの全体構成を示す図である。

【図10】一実施形態におけるDNSサーバ131のハードウェアの構成を示す図である。

【図11】一実施形態において、ウェブサイト装置の接続先を規制するときのフローチャートである。

【図12】一実施形態におけるDNSサーバ131の通信アドレスデータベースを示す図である。

【図1】



*【図13】一実施形態におけるネットワークシステムの全体構成を示す図である。

【図14】一実施形態において、電子メールの送信先を規制するときのフローチャートである。

【図15】一実施形態において、電子メールの送信元を規制するときのフローチャートである。

【図16】一実施形態において、未知機能サーバに対する通信の許可を判定するときのシステム構成を示すものである。

【図17】従来の技術のファイアウォールシステムを示す図である。

【符号の説明】

11, 12, 13・・・クライアント

21・・・メールサーバ

31・・・DNSサーバ

41・・・DNSサーバ

111, 112・・・クライアント

121・・・メールサーバ

131・・・DNSサーバ

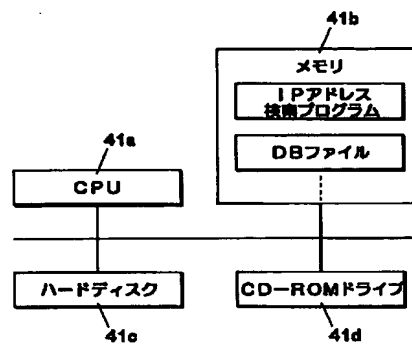
521, 512, 513・・・クライアント

513・・・プロキシサーバ

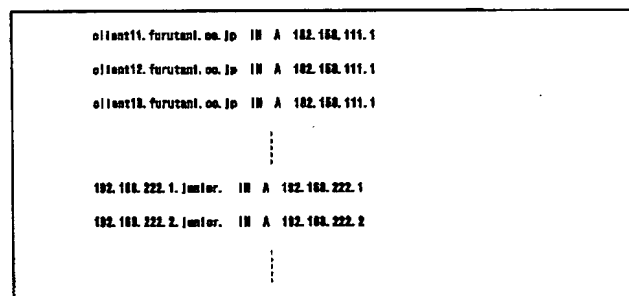
514・・・DNSサーバ

* 521・・・DNSサーバ

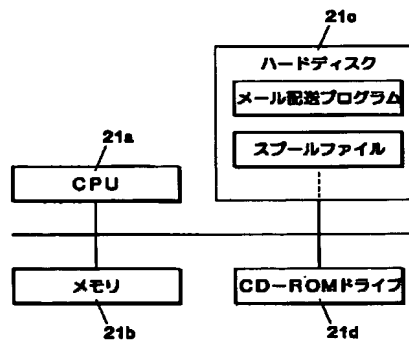
【図2】



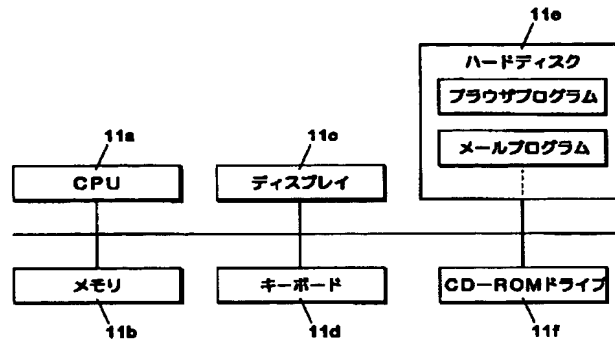
【図3】



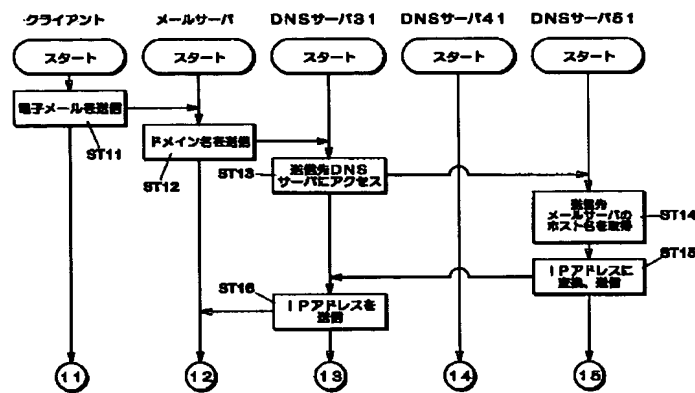
【図4】



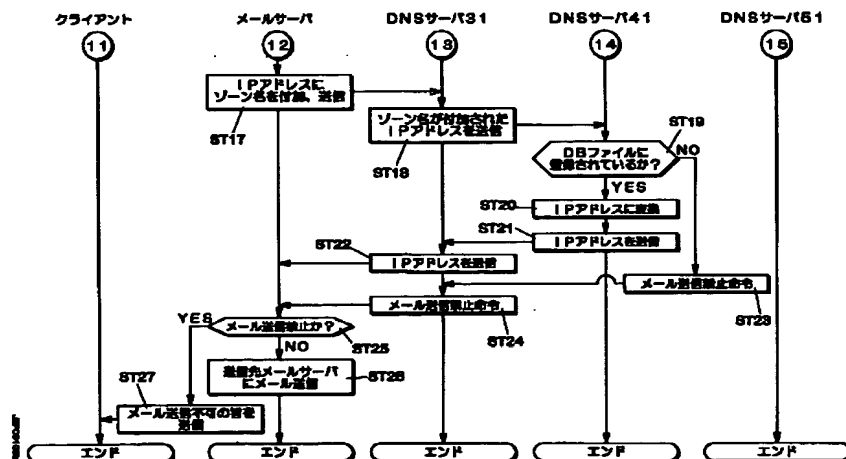
【図5】



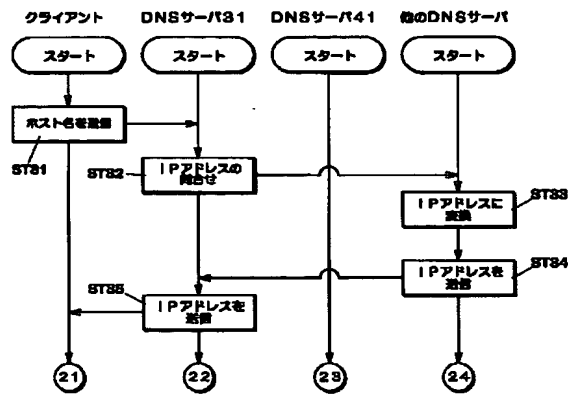
【図6 a】



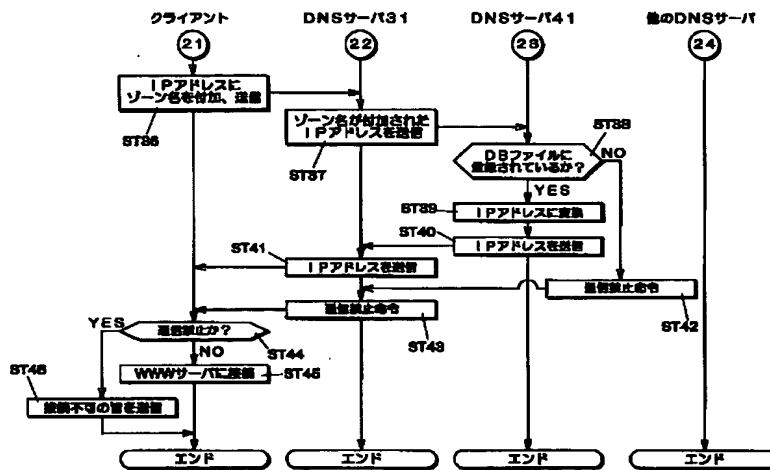
【図6 b】



【図7a】



【図7b】

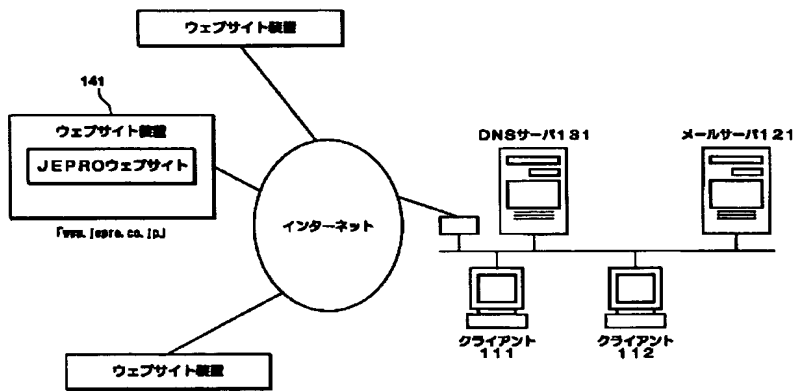


【図8】

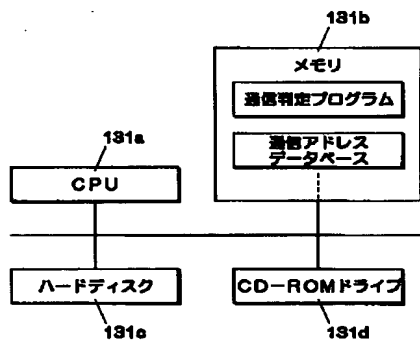
```

192.168.222.1.manager. IN A 192.168.222.1
192.161.162.1.manager. IN A 192.161.162.1
192.161.162.1.teacher. IN A 192.161.162.1
192.141.111.2.manager. IN A 192.141.112.2
192.141.111.2.teacher. IN A 192.141.111.2
192.141.111.2.student. IN A 192.141.111.2
  
```

【図9】



【図10】

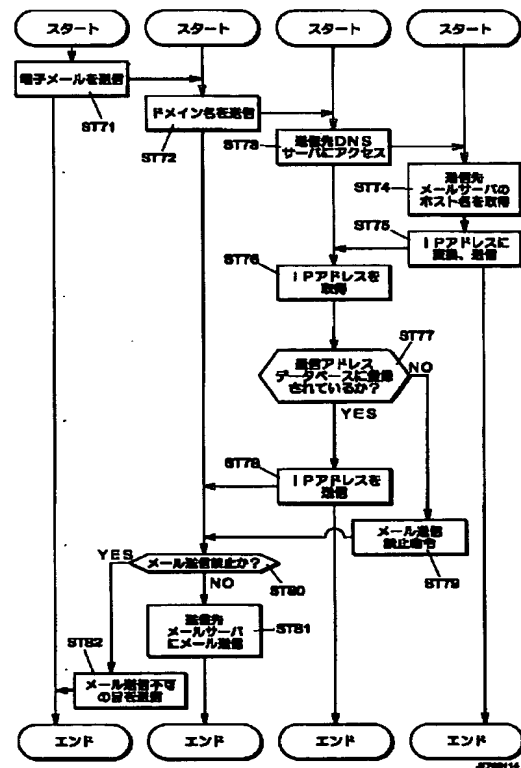


【図12】

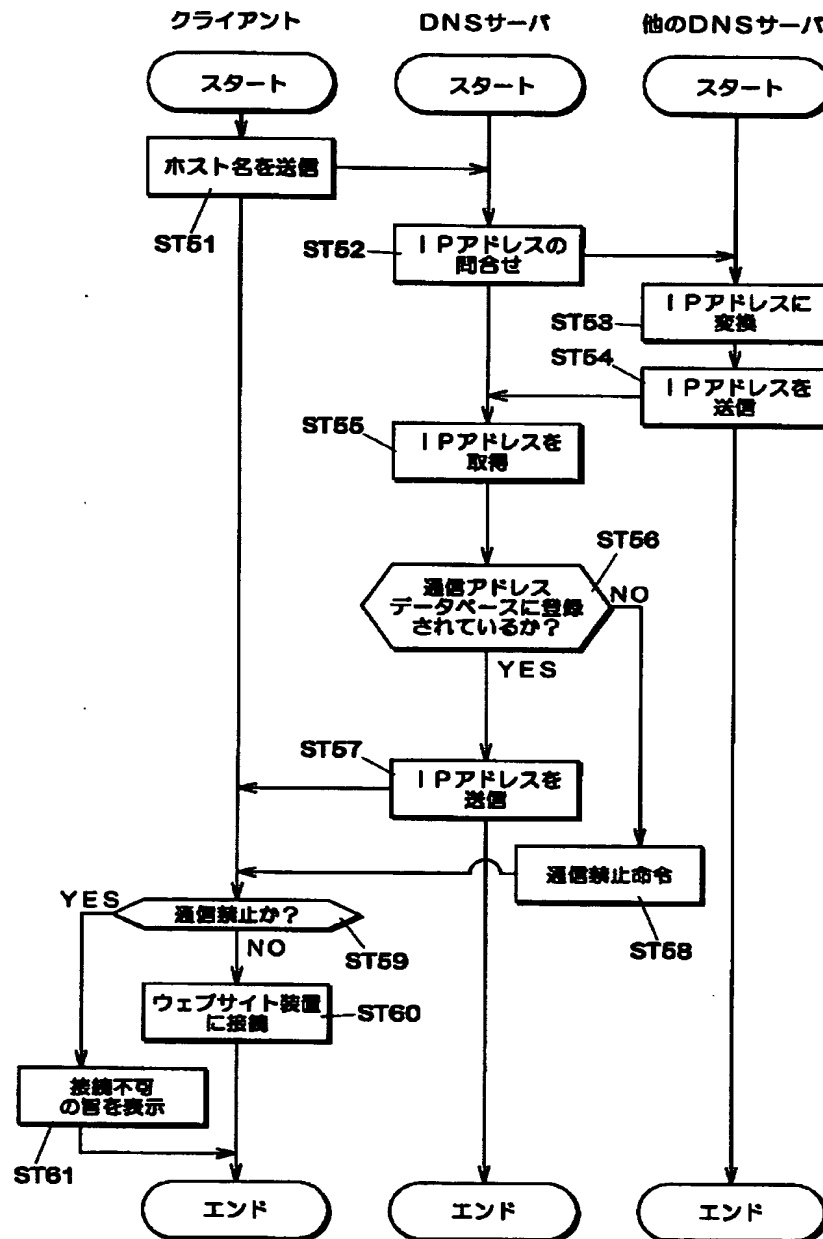
通信アドレスデータベース

192.168.222.1
192.168.222.2
192.168.111.1

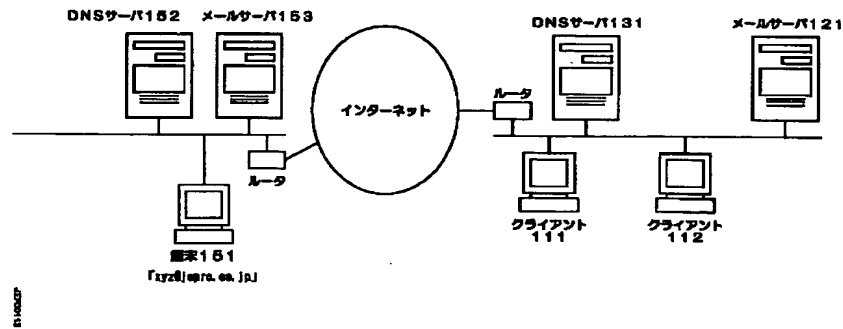
【図14】



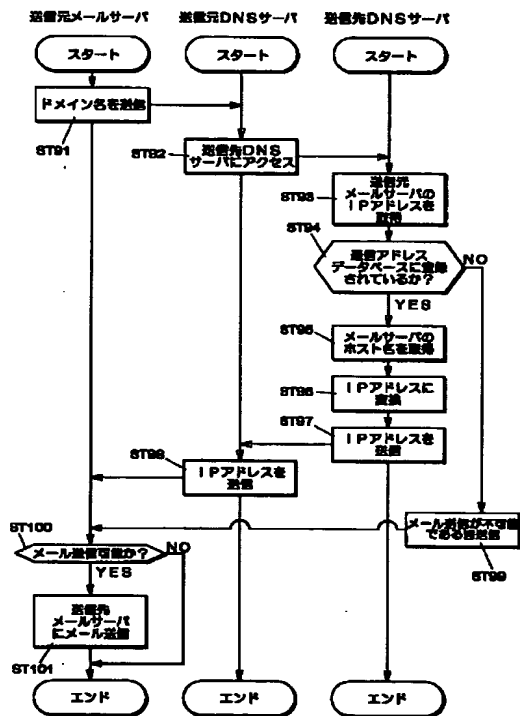
【図11】



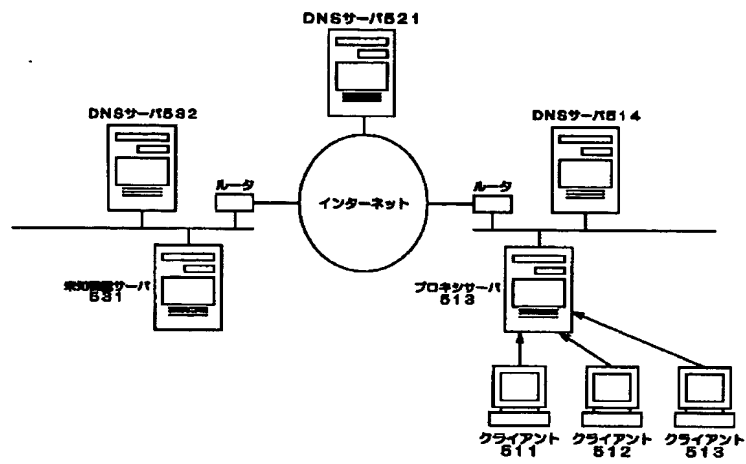
【図13】



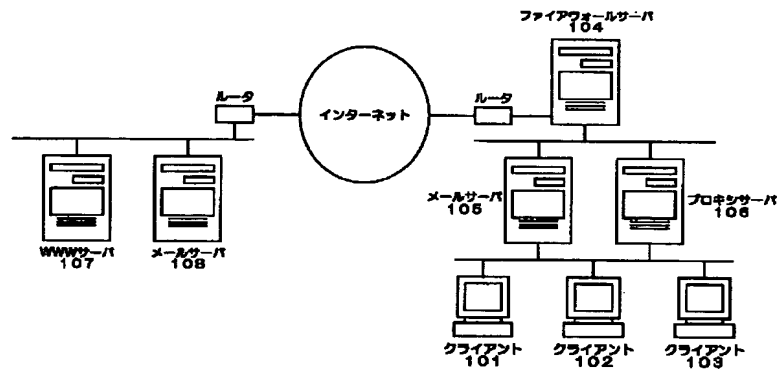
【図15】



【図16】



【図17】



フロントページの続き

F ターム(参考) 5B089 GA11 GA21 GB02 HA10 JA22
 JA31 JB01 JB02 KA17 KB06
 KB13 KC52
 5K030 GA04 GA15 HA06 HB11 HD03
 HD09 JT02